PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 98/13970

(43) International Publication Date: 2 April 1998 (02.04.98)

(21) International Application Number: PCT/US97/17420

(22) International Filing Date: 26 September 1997 (26.09.97)

(30) Priority Data:
08/721,654 26 September 1996 (26.09.96) US

(71) Applicant: WALLENSTEIN & WAGNER, LTD. [US/US]; 311 South Wacker Drive – 5300, Chicago, IL 60606 (US).

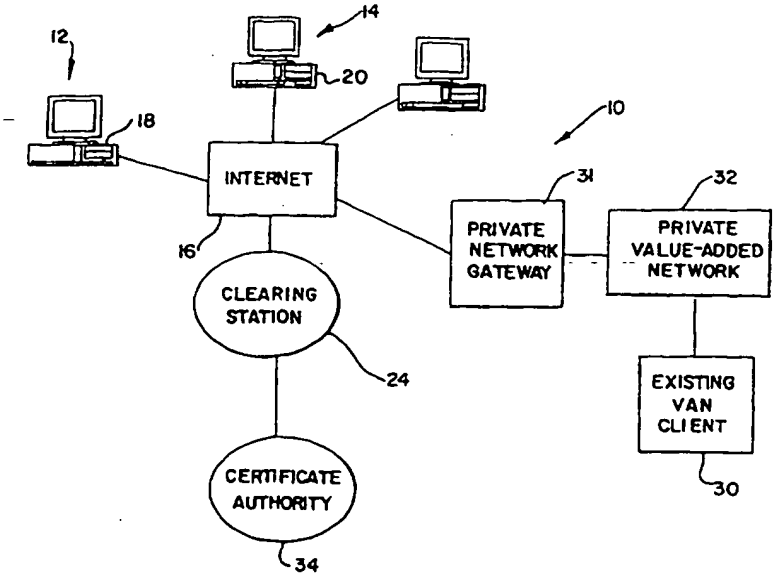
(72) Inventors: PARSONS, Jon, W.; 29 North 700 East, Orem, UT 84097 (US). ANDERSON, Gary, L.; 1135 West 600 North, Orem, UT 84057 (US).

(74) Agents: MORNEAULT, Monique, A. et al.; Wallenstein & Wagner, Ltd., 311 South Wacker Drive – 5300, Chicago, IL 60606 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A SYSTEM AND METHOD FOR SECURELY TRANSFERRING PLAINDATA FROM A FIRST LOCATION TO A SECOND LOCATION



(57) Abstract

The system for securely transferring plaindata (10) from a first location (12) to a second location (14) has a first computer (18) at the first location (12) and a second computer (20) at the second location (14), with the first computer (18) and the second computer (20) being connected to the Internet (16). Through the Internet (16), they are connected to a clearing station (24) and ultimately to a certificate authority (34). In addition, they are connected through the Internet (16) to a private network gateway (31), a private value-added network (32), and an existing van client (30).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

A SYSTEM AND METHOD FOR SECURELY TRANSFERRING PLAINDATA FROM A FIRST LOCATION TO A SECOND LOCATION

DESCRIPTION

Technical Field

The present invention relates to data transfer via a data transport network (the Network), such as a TCP/IP network. The TCP/IP network may be SMTP (Simple Mail Transport Protocol), HTTP (Hypertext Transport Protocol), FTP (File Transfer Protocol), direct IP socket connections, or the like. The present invention relates more particularly to a system and method which provides authentication, non-repudiation, message integrity, confidentiality, and time/date stamping of such data transfer.

Background Prior Art

As electronic commerce, or the transfer of business data such as invoices, via the internet becomes more prevalent, concerns for authentication, non-repudiation, message integrity, confidentiality, and time/date stamping of the data become critical. For example, with electronic commerce, there is no paper trail of the transaction.

The present invention is provided to solve this and other problems.

Summary of the Invention

It is an object of the invention to provide a system for securely transferring a message comprising plaindata from a first location to a second location via a network, such as an SMTP capable transport over a TCP/IP network.

In accordance with the invention, the system comprises a first client station at the first location a second client station at the second location and a clearing station storing key encryption identification information for the second client station. Means are provided for communicatively coupling each of the stations to the network. To transfer the plaindata, means associated with the first client station requests the second client station key encryption identification information from the clearing station via the network. Means responsive to the first client station request transfers the second client station key encryption identification information from the clearing station to the first client station via the network. Means associated with the first client station encrypts the plaindata to form cipherdata utilizing the second client station key encryption identification information. Means then transfers the cipherdata from the first client

station to the second client station via the network. Means transfers transmit confirmation information from the first client station to the clearing station. The transmit confirmation information indicates to the clearing station that the first client station transmitted the cipherdata to the second client station. Means associated with the second client station decrypts the received cipherdata, and means transfers acknowledgement information from the second client station to each of the first client station and the clearing station. The acknowledgement information confirms to the first client station and the clearing station that the second client station received the message.

It is comprehended that the clearing station stores key encryption identification information for the first client station and that the system includes means associated with the second client station for requesting the first client station public key encryption identification information from the clearing station and means responsive to the request for transferring the first client station public key encryption identification information to the second client station.

It is further comprehended that the transmit confirmation information comprises a message number uniquely relating to the plaindata. Alternatively the transmit confirmation information comprises a digest of the plaindata. Still alternatively, the transmit confirmation information comprises the entire plaindata.

It is still further comprehended that the clearing station includes means for providing an audit report of messages sent from the first client station to the second client station.

It is yet further comprehended that the system includes encryption key management, including means for updating encryption identification information.

Other features and advantages of the invention will be apparent from the following specification taken in conjunction with the following drawing.

Brief Description of Drawings

Figure 1 is a block diagram of a first embodiment of the present invention;

Figure 2 is a block diagram of an expanded embodiment of the present invention; and

Figure 3 is a block diagram of a still further expanded embodiment of the present invention.

Detailed Description

While this invention is susceptible of embodiments in many different forms, there is shown in the drawings and will herein be described in detail, preferred embodiments of the invention with the understanding that the present disclosure is to be considered as an exemplification of the principles of the invention and is not intended to limit the broad aspects of the invention to the embodiments illustrated.

A system, generally designated 10, for securely transferring plaindata from a first location 12 to a second location 14 is disclosed in Figure 1. As used herein, the term "plaindata" means data in its state prior to encryption. Typically plaindata is unencrypted, although it is conceivable that encrypted data could be subject to further encryption, and thus such encrypted data would be plaindata. The plaindata is first encapsulated, using a conventional MIME header and trailer. The encapsulated plaindata is then transferred via a data transport network, such as a TCP/IP (Transport Control Protocol/Internet Protocol) network, re-

ferred to herein as internet 16. The network may be SMTP (Simple Mail Transport Protocol), or conventional e-mail). Alternatively, the plaindata can be transferred via HTTP (Hypertext Transport Protocol), FTP (File Transfer Protocol), direct IP socket connections, or the like.

The system comprises a first client station 18 at the first location and a second client station 20 at the second location. The first client station 18 and the second client station 20 are anticipated to be conventional personal computers, or PC's, having respective modems (not specifically shown) connected to a conventional telephone network. The connection to the telephone network may be direct, or over a network such as a local area network.

The system 10 further includes a clearing station 24. The clearing station 24 can also be a conventional PC having a modem connecting the clearing station 24 via a telephone network to the internet 16.

As is well known, there are two conventional models of data encryption, symmetric and asymmetric.

According to symmetric data encryption, a single digital number, or key, is used both to encrypt and decrypt plaindata.

According to asymmetric data encryption, two related digital numbers are used. The first number is commonly referred to as a public key and the second number is commonly referred to as a private key. An entity maintains its private key private, as the name suggests, and makes its public key known to those needing it. If the first entity is to send plaindata to a second entity, the first entity encrypts the plaindata into cipherdata using

the second entity's public key. The second entity then decrypts the received cipherdata into plaindata using its own private key. Thus once plaindata is encrypted with the second entity's public key, only the holder of the second entity's private key can decrypt the cipherdata. A more complete discussion of data encryption schemes can be found in Computer Communication Security, by Warwick Ford, Prentiss-Hall, 1994. Another reference is Applied Cryptography, by Bruce Schneier, published by Counterpane Systems, Oak Park, IL.

The clearing station 24 stores key encryption identification information for the second client station. The key encryption identification information would be the second client station's only key, if symmetric encoding was being utilized, or the key encryption identification information would be the second client station's public key, if asymmetric encoding was being utilized. As noted above, each of the stations 18, 20, 24 is communicatively coupled to the internet 16.

The following is a discussion describing how plaindata is transferred from the first client station 18 to the second client station 20. Software operable by the first client station 18 causes the first client station 18 to contact the clearing station 24 via the internet 16 and requests the second client station key encryption identification information from the clearing station 24. The clearing station 24 automatically responds to the first client station request and transfers the second client station key encryption identification information from the clearing station 24 to the first client station 18 via the internet 16.

The first client station 18 then encrypts the plaindata to be sent to the second client station

20 to form cipherdata. This encryption utilizes the second client station key encryption identification information. Once encrypted, the first client station 18 then automatically transfers the cipherdata from the first client station 18 to the second client station 20 via the internet 16. In addition, the first client station 18 automatically transfers transmit confirmation information from the first client station 18 to the clearing station 24. The transmit confirmation information indicates to the clearing station 24 that the first client station 18 transmitted the cipherdata to the second client station 20.

After the second client station 20 receives the cipherdata from the first client station 18, the second client station utilizes conventional software to decrypt the received cipherdata. In addition, the second client station 20 automatically transfers acknowledgement information from the second client 20 station to each of the first client station 18 and the clearing station 24. The acknowledgement information confirms to the first client station 18 and the clearing station 24 that the second client station 20 received the plaindata. This provides for bi-lateral non-repudiation of the message.

In the preferred embodiment, the clearing station 24 stores key encryption identification information for the first client station 18. Accordingly the second client station 20 would automatically request the first client station key encryption identification information from the clearing station 24 and the clearing station 24 would respond to the request and transfer the first client station key encryption identification information to the second client station 20. The second

client station 20 would use the first client station key encryption identification information to unencrypt the message digest of the cypherdata from the first client station 18. The first client station key encryption identification information is also used by the second client station 20 to encrypt any plaindata the second client station 20 would send in response to the first client station 18.

The transmit confirmation information may comprise a message number uniquely relating to the plaindata. Alternatively the transmit confirmation information may comprise a digest of the plaindata. Still alternatively, the transmit confirmation information may comprise the entire plaindata.

Over the course of time, the confidentiality of a key may be questioned, and thus the holder of the key may desire the number to be changed. Accordingly the key identification information stored at the clearing station 24, and hence provided to the client stations, can be updated. Additionally, the key identification information stored at the clearing station 24, and hence provided to the client stations, can be automatically updated on a periodic basis.

In addition, a transaction between parties may be challenged. Accordingly, the clearing station 24 providing an audit report of messages sent from the first client station 18 to the second client station 20.

The above discussion related to data transfer from the first client station 18 to the second client station 20. It is intended that similar data transfer may be made from the second client station 20 to the first client station 18. Still further, similar data transfer may be made between

an EDI system 30 coupled to the internet 16 via a private network gateway 31 and a private value added network 32 (such as CompuServ) and either of the first client station 18 and/or the second client station 20.

As is well known, a digital certificate can be used with asymmetric encryption to authenticate both that the identified sender is in fact the true sender and that the message was not altered. Accordingly, the sender utilizes a "hashing algorithm" (typically either MD-3 or MD-5 protocols) to transform plaindata to be sent into a "message digest." The "message digest" is then encrypted by the sender using the sender's private key. The encrypted message digest, is called the digital certificate, and is attached to the encrypted message and sent to the receiver. The receiver uses the receiver's private key to decrypt the encrypted message. The receiver also uses the sender's public key to decrypt the encrypted message digest, and then uses the hashing function to reform the decrypted message digest to the original message. If the message as reformed from the message digest is the same as the decrypted message as sent, then one knows that the true sender sent the message.

In accordance with the invention, a certificate authority 34, such as VeriSign, Inc., of Mountain View, California, creates and manages digital certificates and signatures. The particulars of a certificate authority are discussed by Ford, referenced above.

An expanded version of the invention is illustrated in Figure 2. According to this version, first and second clearing stations 24, 24', and their respective first, second, third and fourth

client stations 18, 20, 18', 20' are interconnected by an internet connection between the respective clearing stations 24, 24'. According to this version, if the first client station 18 of the first clearing station 24 desires to transfer plaindata to the fourth client station 20' of the second clearing station 24', the first client station 18 requests the key identification information of the fourth client station 20' via the first and second clearing stations 24, 24'. Thus both clearing stations are required to get the key identification information to the first client station 24. Once the first client station has the key identification information, the plaindata is transferred as discussed above, utilizing the first clearing station for verification.

A still further expanded version of the invention is illustrated in Figure 3. According to this version, first and second clearing stations 24, 24', and their respective first, second, third and fourth client stations 18, 20, 18', 20' are interconnected by a commerce broker 36 between the respective clearing stations 24, 24'. The commerce broker 36 is utilized when a direct connection between clearing stations is not desired, such as when a bank's computer and a bulletin board service are each "clearing stations", and the bank does not want a direct connection with the bulletin board service. Accordingly, a mutually trusted entity is selected to act as the commerce broker 36.

The system 10 operates in conjunction with conventional Windows® based software products, such as accounting systems, spreadsheets, word processing, inventory control, e-mail, or the like, using Windows® API (application program interface). It will be understood that the invention may be embo-

died in other specific forms without departing from the spirit or central characteristics thereof. The present examples and embodiments, therefore, are to be considered in all respects as illustrative and not restrictive, and the invention is not to be limited to the details given herein.

CLAIMS

1. A system for securely transferring plaindata from a first location to a second location via a data transport network, the system comprising:

a first client station at said first location;

a second client station at said second location;

a clearing station storing key encryption identification information for said second client station;

means for communicatively coupling each of said stations to said network;

means associated with said first client station for requesting said second client station key encryption identification information from said clearing station via said network;

means responsive to said first client station request for transferring said second client station key encryption identification information from said clearing station to said first client station via said network;

means associated with said first client station for encrypting said plaindata to form cipherdata utilizing said second client station key encryption identification information;

means for transferring said cipherdata from said first client station to said second client station via said network;

means for transferring transit confirmation information from said first client station to said clearing station, said transmit confirmation information indicating to said clearing station that said first client station transmitted said cipherdata to said second client station;

means associated with said second client station for decrypting said received cipherdata; and

means for transferring acknowledgement information from said second client station to each of said first client station and said clearing station, said acknowledgement information confirming to said first client station and said clearing station that said second client station received said plaindata.

2. The system of claim 1 wherein said clearing station stores key encryption identification information for said first client station and said system includes means associated with said second client station for requesting said first client station public key encryption identification information from said clearing station and means responsive to said request for transferring said first client station public key encryption identification information to said second client station.

3. The system of claim 1 wherein said transmit confirmation information comprises a message number uniquely relating to said plaindata.

4. The system of claim 1 wherein said transmit confirmation information comprises a digest of said plaindata.

5. The system of claim 1 wherein said transmit confirmation information comprises the entire plaindata.

6. The system of claim 1 wherein said clearing station includes means for providing an audit report of plaindata sent from said first client station to said second client station.

7. The system of claim 1 including means for updating encryption identification information.

8. A system for securely transferring plaindata from a first location to a second location via an SMTP capable transport over a TCP/IP network, the system comprising:

a first client station at said first location;

a second client station at said second location;

a clearing station storing key encryption identification information for said second client station;

means for communicatively coupling each of said stations to said network;

means associated with said first client station for requesting said second client station key encryption identification information from said clearing station via said network;

means responsive to said first client station request for transferring said second client station key encryption identification information from said clearing station to said first client station via said network;

means associated with said first client station for encrypting said plaindata to form cipherdata utilizing said second client station key encryption identification information;

means for transferring said cipherdata from said first client station to said second client station via said network;

means for transferring transit confirmation information from said first client station to said clearing station, said transmit confirmation information indicating to said clearing station that said first client station transmitted said cipherdata to said second client station;

means associated with said second client station for decrypting said received cipherdata; and

means for transferring acknowledgement information from said second client station to each of said first client station and said clearing station, said acknowledgement information confirming to said first client station and said clearing station that said second client station received said plaindata.

9. The system of claim 8 wherein said clearing station stores key encryption identification information for said first client station and said system includes means associated with said second client station for requesting said first client station public key encryption identification information from said clearing station and means responsive to said request for transferring said first client station public key encryption identification information to said second client station.

10. The system of claim 8 wherein said transmit confirmation information comprises a message number uniquely relating to said plaindata.

11. The system of claim 8 wherein said transmit confirmation information comprises a digest of said plaindata.

12. The system of claim 8 wherein said transmit confirmation information comprises the entire plaindata.

13. The system of claim 8 wherein said clearing station includes means for providing an audit report of plaindata sent from said first client station to said second client station.

14. The system of claim 8 including means for updating encryption identification information.

15. A system for securely transferring plaindata from a first location to a second location via an SMTP capable transport over a TCP/IP network, the system comprising:

a first client station at said first location;

a second client station at said second location, said second client station for storing private key encryption identification information for said second client station;

a clearing station a for storing public key encryption identification information for said second client station, said public key encryption identification information corresponding to said private key encryption identification information;

means for communicatively coupling each of said stations to said network;

means associated with said first client station for requesting said second client station public key encryption identification information from said clearing station via said network;

means responsive to said first client station request for transferring said second client station public key encryption identification information from said clearing station to said first client station via said network;

means associated with said first client station for encrypting said plaindata to form cipherdata utilizing said second client station public key encryption identification information;

means for transferring said cipherdata from said first client station to said second client station via said network;

means for transferring transit confirmation information from said first client station to said clearing station, said transmit confirmation information indicating to said clearing station that

said first client station transmitted said cipher-data to said second client station;

means associated with said second client station for utilizing said second client station private key for decrypting said received cipher-data; and

means for transferring acknowledgement information from said second client station to each of said first client station and said clearing station, said acknowledgement information confirming to said first client station and said clearing station that said second client station received said plaindata.

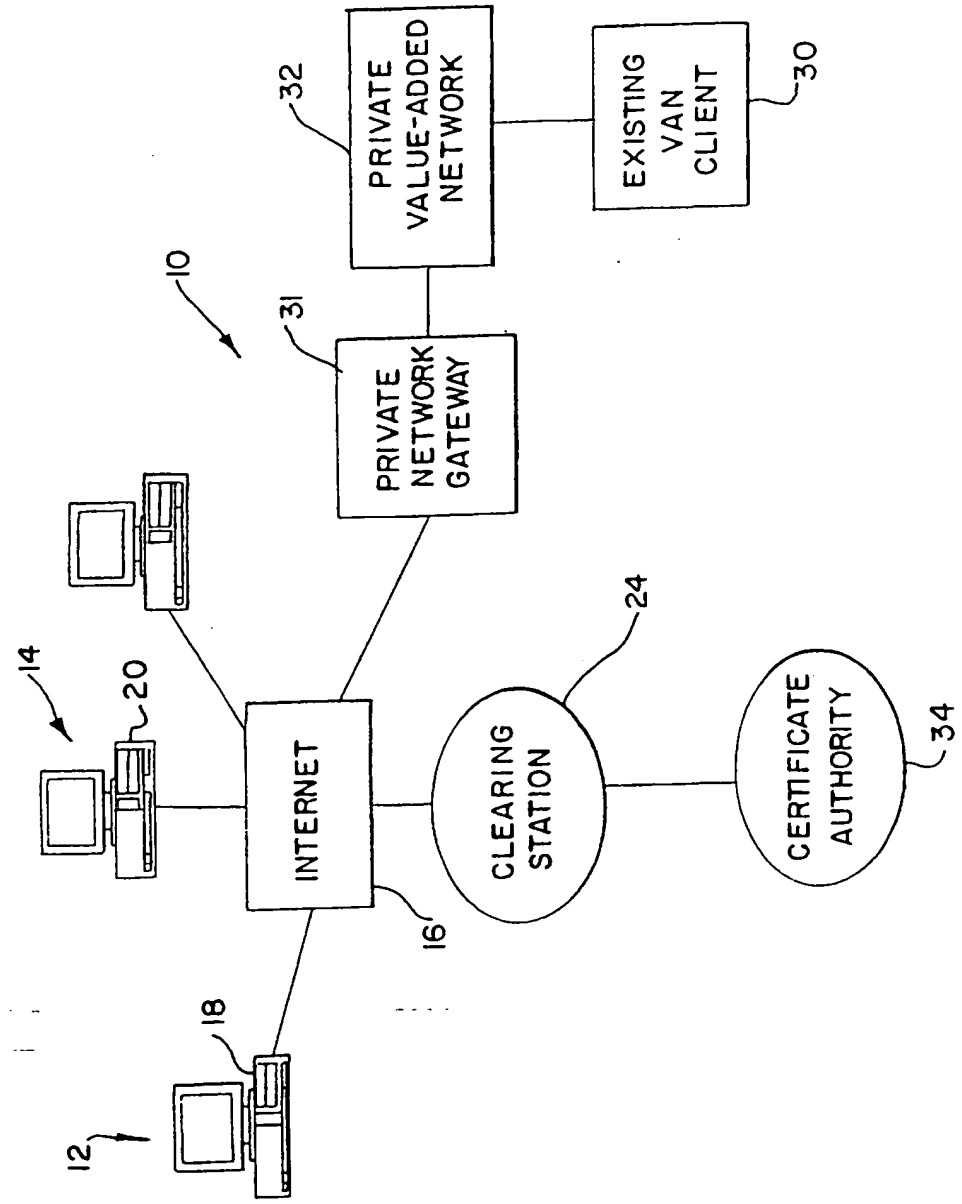


FIG.1

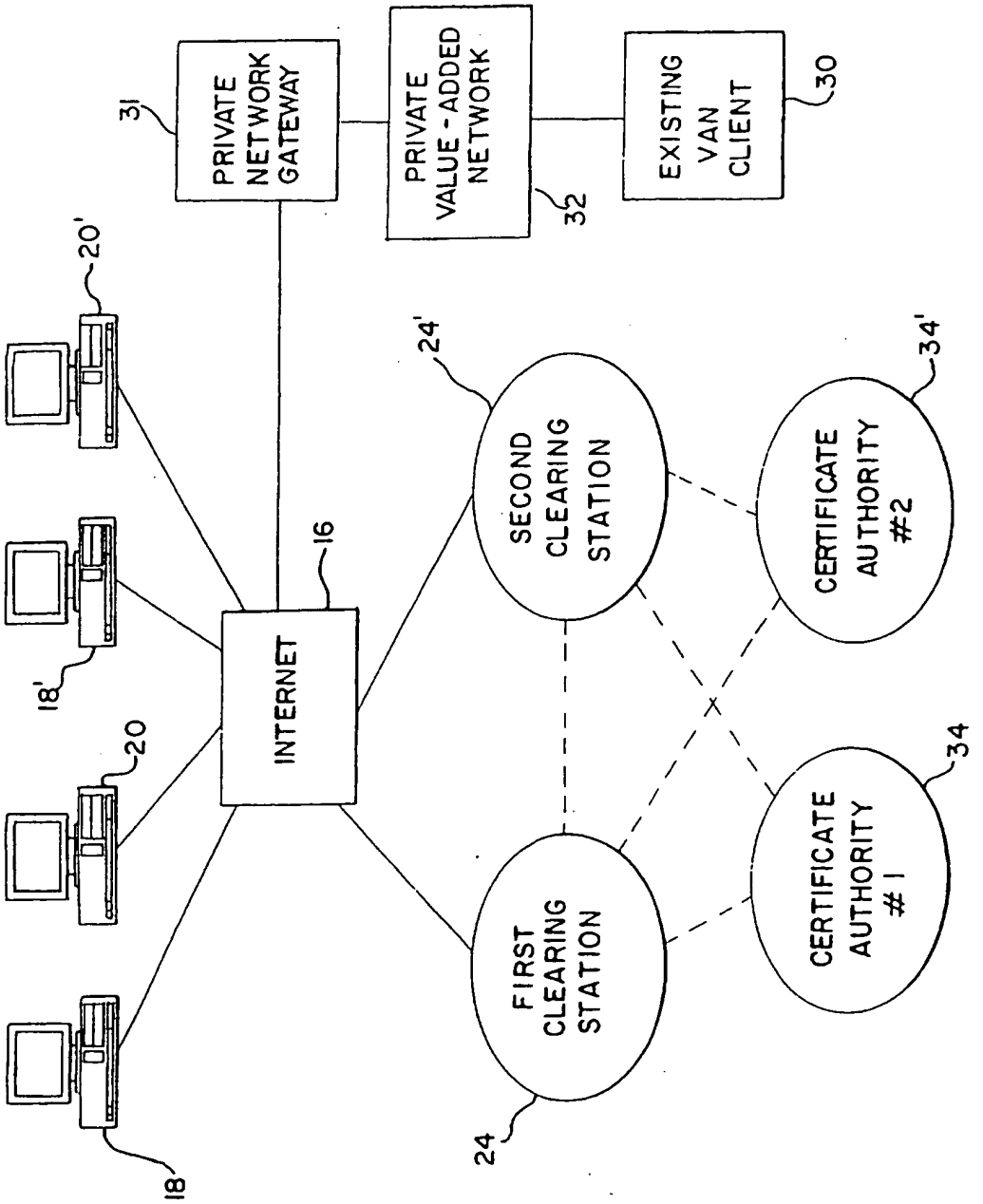
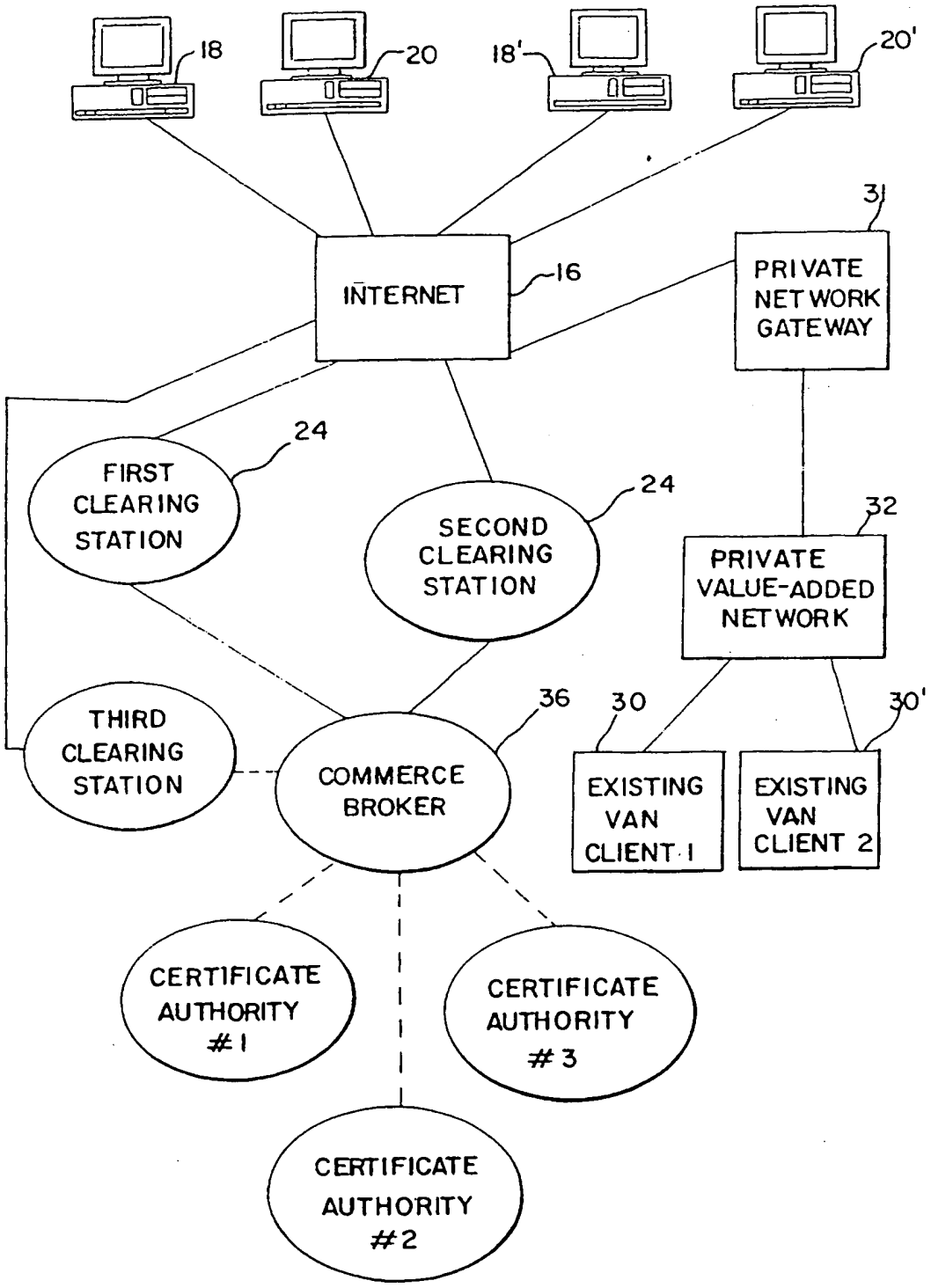


FIG. 2

FIG. 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/17420

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL : 380/23

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 21, 30, 4, 9, 24, 25, 49, 50, 59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,182,933 A (ROSENBLUM) 08 January 1980, see abstract.	1-15
A	US 4,578,532 A (MARKWITZ) 25 March 1986, see abstract.	1-15
A	US 4,866,707 A (MARSHALL et al) 12 September 1989, see abstract.	1-15
A	US 5,146,497 A (BRIGHT) 08 September 1992, see abstract.	1-15
A	US 5,150,408 A (BRIGHT) 22 September 1992, see abstract.	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

20 NOVEMBER 1997

Date of mailing of the international search report

13 JAN 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

BERNARR EARL GREGORY

Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*